

UNITED STATES DISTRICT COURT

for the
District of ColoradoIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 12-sw-05575-MJW

8861 E. Florida Avenue, Apartment B110, Denver,
Colorado, 80247 more fully described in Attachment
A, attached hereto.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the State and District of Colorado, there is now concealed (identify the person or describe the property to be seized):

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section18 U.S.C. § 1425 (a) and (b)
18 USC §§ 1028(a)(3), (4), (7)18 USC §§ 1028A
18 USC § 1546(a)**Offense Description**Unlawful Procurement of Citizenship/Naturalization
Fraud and related activity in connection with
identification documents and information
Aggravated identity theft
Fraud and misuse of visas, permits, and other documents

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

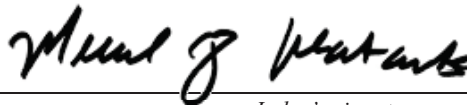
s/Jeffrey Lembke

Applicant's signature

Special Agent Jeffrey Lembke, HS/JICE

Printed name and title

Sworn to before me and signed in my presence.

Date: 23 Aug 2012City and state: Denver, CO

Judge's signature

Michael J. Watanabe
U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The property to be searched is located at 8861 E. Florida Avenue, Apartment B110, Denver, Colorado, 80247 within the Sierra Vista apartment complex. The Sierra Vista apartment complex is comprised of four multi-unit, residential buildings each with its own street address.

The building located at 8861 E. Florida Avenue is clearly marked with the numbers “8861.” It has three levels. The building has brown stucco siding and, of the four buildings, it is situated the furthest north and east.

Apartment B110 is located on the second floor of the building located at 8861 E. Florida Avenue and is clearly marked with the numbers “110” in approximately 4 inch high black numbers. To get to Apartment B110, you enter the building located at 8861 E. Florida Avenue, Denver, Colorado at the building’s east main entry and travel up one flight of stairs. At the first floor, you turn north and apartment is B110 is on the east side of the hallway.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

The following items, located within the residence at Subject Premises, that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of Title 18, United States Code, Sections 1425(a) and (b), 1028(a)(3), (4), (7), 1028A and 1546(a).

1. Any document or papers, genuine or counterfeit, reflecting identity, immigration status and citizenship, including but not limited to passports, alien registration cards, I-94 Departure/Arrival records, certificates of naturalization, birth certificates, foreign or domestic driver's licenses, social security cards, and all identity documents bearing the name Habteab Berhe Temanu or Kefelegn Alemu Worku (or variations of the name Kefelegn Alemu Worku).
2. All other documents bearing the name name Habteab Berhe Temanu or Kefelegn Alemu Worku (or variations of the name Kefelegn Alemu Worku) including but not limited to bank account statements, utility bills, telephone bills, cable bills, lease agreements, immigration applications, employment documents, and credit card statements.
3. All documents which are deemed to be evidence of "Temanu's" real identity to include documents bearing alternate identities, address books, contact lists, photographs, and correspondence.
4. Any and all notes, software, documents, records, or correspondence, electronic mail, memorandum or any written or oral communication in any format and medium pertaining to violations of Title 18, United States Code, 1425(a) and (b), 1028(a)(3), (4), (7), 1028A and 1546(a).
5. Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, digital storage media, any physical object upon which computer data can be recorded, gaming devices, digital communications devices, cellular telephones, cameras, videotapes, video recording devices, video recording players, an video display monitors, digital input and output devices such as keyboards, mouse(s), scanners, printers, monitors, electronic media and network equipment, modems, routers, connection and power cords, and external or connected devices used for accessing computer storage media that was used to commit or facilitate commissions of Title 18, United States Code, Sections 1425(a) and (b), 1028(a)(3), (4), (7), 1028A and 1546(a).
6. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, COMPUTER) that is called for by this warrant, or that might contain items otherwise called for by this warrant:
7. All electronic media capable of storing the above outlined evidence to include computers, external hard drives, digital storage media, thumb drives, compact disks, DVDs, and cell phones containing evidence of, contraband, the fruits of crime, or used to facilitate commissions of Title 18, United States Code, Sections 1425(a) and (b), 1028(a)(3), (4), (7), 1028A and 1546(a).

8. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, COMPUTER) that is called for by this warrant, or that might contain items otherwise called for by this warrant:
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, user profiles, e-mail, e-mail contacts, "chat" or instant messaging logs, photographs, and correspondence;
 - b. evidence of software that may allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;
 - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. contextual information necessary to understand the evidence described in this attachment;
 - j. any and all information, notes, software, documents, records, or correspondence, in any format and medium pertaining to violations of Title 18, United States Code, Sections 1425(a) and (b), 1028(a)(3), (4), (7), 1028A and 1546(a).
 - k. items otherwise described above in paragraphs 1- 5 of this Attachment B.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent Jeffrey Lembke, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge and belief:

1. I am a special agent with Homeland Security Investigations (HSI), Immigration and Customs Enforcement (ICE). I am currently assigned to the Special Agent in Charge, Denver, Colorado. I have been a special agent for approximately sixteen (16) years. Prior to the formation of the Department of Homeland Security (DHS) in March of 2003, I was employed as a special agent of the United States Immigration and Naturalization Service (INS) and the United States Customs Service (USCS). I have successfully completed the Immigration Officer Basic Training and the Customs Basic Enforcement School at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia. I have also completed numerous post academy training courses in laws relating to the Immigration and Nationality Act to include training in methods and schemes employed by foreign nationals to circumvent the immigration laws.
2. This affidavit is submitted in support of an application for a search warrant for the residence of 8861 E. Florida Avenue, Apartment B110, Denver, Colorado, 80247 (hereinafter "Subject Premises"), and any computer(s) located therein, for evidence of violations of Title 18 United States Code, Section 1425(a) and (b) [Procurement of Naturalization Unlawfully], Title 18, United States Code, Section 1028(a)(3), (4), (7)[Fraud and related activity in connection with identification documents and information],], Title 18, United States Code, Section 1028A [Aggravated Identity Theft] and Title 18, United States Code, Section 1546(a)[Fraud and misuse of visas, permits, and other documents]. The Subject Premises is more fully described in Attachment A.
3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Section 1425(a) and (b) [Procurement of Naturalization Unlawfully], Title 18, United States Code, Section 1028(a)(3), (4), (7)[Fraud and related activity in connection with identification documents and information],], Title 18, United States Code, Section 1028A [Aggravated Identity Theft] and Title 18, United States Code, Section 1546(a)[Fraud and misuse of visas, permits, and other documents], are presently located at the Subject Premises.
4. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

RELEVANT STATUTES

5. Title 18 United States Code, Section 1425(a) and (b) prohibits: (a) knowing procurement or attempted procurement, contrary to law, of the naturalization of any person, or documentary or other evidence of naturalization or of citizenship; or (b) whether for himself or another person not entitled thereto, knowing issuance, procurement or obtaining or applying for or otherwise attempting to procure or obtain naturalization, or citizenship, or a declaration of intention to become a citizen, or a certificate of arrival or any certificate or evidence of nationalization or citizenship
6. 18 U.S.C. § 1028(a) makes it a criminal offense for any person to knowingly (3) possess with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents; (4) possess an identification document, authentication feature, or false identification document, with the intent that such document or feature be used to defraud the United States; and (7) transfer, possess, or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.
7. 18 U.S.C. § 1028A makes it a criminal offense to, during and relation to various felony offenses including Chapter 69, relating to nationality and citizenship, and Chapter 75, relating to passports and visas, knowingly transfer, possess, or use, without lawful authority, a means of identification of another.
8. 18 U.S.C. § 1546(a) prohibits a person from knowingly forging, counterfeiting, altering, or falsely making any immigrant or nonimmigrant visa, permit, border crossing card, alien registration receipt card, or other document prescribed by statute or regulation for entry into or as evidence of authorized stay and employment in the United States and from uttering, using, attempting to use, possessing, obtaining, accepting, or receiving any such visa, permit, border crossing card, alien registration receipt card, or any other document prescribed by statute or regulation for entry into or as evidence of authorized stay or employment in the United States, knowing it to be forged, counterfeited, altered, or falsely made, or to have been procured by means of any false claim or statement, or to have been otherwise procured by fraud or unlawfully obtained.

SEIZURE AND SEARCH OF COMPUTERS

9. As described above and in Attachment B, I submit that if computers or storage media are found at the Subject Premises, there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

10. For example, based on my knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks, floppy, tape and/or CD-ROM and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value are lost when a computer is powered-off and unplugged.
11. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space--that is, in space on the storage medium that is not currently being used by an active file--for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
12. Also, again based on my training and experience, wholly apart from user-generated files, computer storage media--in particular, computers' internal hard drives--contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
13. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.
14. In cases like this one, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all

related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

15. In cases of this sort, the computer and its storage devices, the mouse, the monitor, keyboard, printer, modem and other system components are also used as instrumentalities of the crime to operate the computer. Devices such as modems can contain information about dates, frequency, and computer(s) used to access the internet. The monitor, keyboard, and mouse may also have fingerprints on them indicating the user of the computer and its components.
16. Similarly, files related to an individual's true identity found on computers and other digital communications devices are usually obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.
17. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
18. Your Affiant knows from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.
19. Searching Computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. Or, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly

organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

20. Based upon my knowledge, training and experience, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:
 - a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.
 - b. The volume of evidence and time required for an examination. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
 - c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

INVESTIGATION

22. In May 2011, HSI received information from a naturalized United States citizen originally a native of Ethiopia (hereinafter referred to as “KK”). In May 2011, “KK”, a resident of Denver, Colorado, reported that he had recently encountered a person in Denver whom he recognized as Kefelegn ALEMU WORKU, a prison guard during a period in the late 1970’s in Ethiopia known as the “Red Terror.”
23. Your affiant has learned that in the late 1970’s in Ethiopia, Mengistu Haile Mariam rose to assume unofficial control of the Provisional Military Administrative Committee (PMAC) also known as the Dergue. The Dergue was a committee of nearly 120 military officers, that, once it came to power in the mid-1970’s as a Marxist regime, abolished Ethiopia’s Constitution and arrested the former emperor and members of the imperial government for alleged crimes against the Ethiopian people. During this time, Mengistu commanded the execution of nearly 60 former government officials. Mengistu seized full control in 1977 which unleashed a two-year campaign in Ethiopia known as the “Red Terror.” During the Red Terror tens of thousands of Ethiopian men, women, and children suspected of being members or supporters of the anti-Dergue revolutionary group known as the Ethiopian People’s Revolutionary Party (EPRP) were arrested, tortured, and summarily executed. Those individuals who were detained were incarcerated in government prisons with deplorable conditions including being packed by the hundreds into airless, lightless cellars, where they could hear the screams of those being tortured while they awaited torture themselves. One such prison was known as “Kebele 15” or “Kefetegna 15” which in English roughly translates as “Higher 15.” The “Higher 15” prison housed approximately 1500 prisoners who had been imprisoned due to their political opinions and affiliations. During the Red Terror, families of the killed or missing were often required to pay the government for the bullet used to kill the family member before the body would be released for burial. It is not known how many people were killed, imprisoned, or forced to flee Ethiopia during the Red Terror campaign, but historical accounts indicate that a minimum of 10,000 people were killed in the city of Addis Ababa alone in 1977 with probably comparable numbers in the provinces in 1977 and 1978.
24. “KK” explained that he had become a political prisoner in Ethiopia in February 1978 when he was arrested and sent to a makeshift neighborhood prison known as the “Higher 15” or “Kebele 15.” There, “KK” witnessed ALEMU WORKU torture fellow prisoners

and learned that other prisoners were being executed at the hands of prison guards, including ALEMU WORKU. “KK” was held at the “Higher 15” until he managed to escape in September 1979.

25. “KK” provided Colorado license plate 472 OVL as relating to the person he had recognized as ALEMU WORKU. Your affiant learned that license plate 472 OVL is registered to Habteab B. TEMANU at 8861 E. Florida Avenue, Apartment B110, Denver, Colorado. Immigration records confirm that “Habteab Berhe TEMANU” is a naturalized United States citizen from Ethiopia and he is assigned alien registration number A94 666 247. “KK” was shown a photographic lineup display which included the photograph of “TEMANU” and five other men of similar physical characteristics and he indicated that he was “100 percent certain” that “Habteab Berhe TEMANU” is Kefelegn ALEMU WORKU.
26. A review of alien file A94 666 247 relating to “Habteab Berhe TEMANU” showed that he immigrated to the United States on July 12, 2004 as a refugee along with four of his purported children, Y.B., A.B., M. B., and T.B.. During the refugee application process, “TEMANU” claimed that he had fled with his children from Ethiopia and travelled to Nairobi, Kenya in 2000 due to the conflict between Ethiopia and Eritrea. He claimed he had been arrested in Nazareth, Ethiopia because of his Eritrean ethnicity and that the government of Ethiopia accused him of helping the Eritrean government. Documents in the file show that “TEMANU” and the children were sponsored by a fifth child, S.B., who immigrated to the United States in 1995 through the diversity visa program. The Diversity Immigrant Visa Program makes diversity visas available annually to randomly selected eligible applicants from countries with low rates of immigration to the United States.
27. S.B. began the process of attempting to gather his family in the United States in approximately August of 2000 by filing, through a charitable organization, a document known as an Affidavit of Relationship with the Legacy Immigration and Naturalization Service (INS).¹ The Affidavit of Relationship is the form used to reunite refugees and asylees with close relatives who are determined to be refugees but are outside the United States.
28. On November 29, 2006, “TEMANU” filed Form I-485, Application to Register Permanent Residence or Adjust Status. In the application, “TEMANU” identified his family as including the five children discussed above. “TEMANU” also identified an additional daughter born in Kenya in 2001 named “Aklesiya.” As evidence of identity, “TEMANU” provided copies of his I-94 Arrival/Departure record, Colorado driver’s license, PIN 04-201-0745, and social security account card number, 651-32-9064. On January 19, 2008, “TEMANU’s” Form I-485 was approved and he was granted permanent residency in the United States and issued a Permanent Resident Card.

¹The INS was abolished in 2003. In its place the U.S. Department of Homeland Security (DHS) was created. Within DHS is U.S. Citizenship and Immigration Services (USCIS), which administers immigration benefits and U.S. Immigration and Customs Enforcement (ICE), whose mission includes the enforcement of criminal and administrative immigration law.

29. On November 22, 2009, "TEMANU" filed Form N-400, Application For Naturalization, in which he submitted the same biographic and family information. On March 2, 2010, "TEMANU's" application for citizenship was approved and "TEMANU" was granted United States citizenship. He was issued Certificate of Naturalization number 32776687.
30. In June 2011, I obtained an open source news article entitled "Genocide Convict Sentenced to Death in Absentia" dated March 17, 2001. The article stated that "the Sixth Central Bench of the Federal High Court has sentenced a genocide suspect to death and 26 others to various jail terms ranging from two years up to life in prison. The court said the convicts were among the 50 individuals accused of perpetrating extra-judicial killings while serving under the defunct military regime at various positions in the former Higher 15 metropolis. Kefelegn ALEMU, who received the death penalty in absentia, was found guilty of ordering, coordinating and participating in the execution of 101 people, the court said. The death penalty would be carried out by hanging the convict after being approved by the head of state." Efforts to obtain official documentation from the government of Ethiopia relating to the above referenced trial and "Kefelegn ALEMU" are ongoing.
31. On July 15, 2011, a naturalized United States citizen originally from Ethiopia (hereinafter referred to as "NS"), was interviewed by HSI special agents in Sterling, Virginia. "NS" stated that he was imprisoned in the Higher 15 from December 1977 to December 1978. At that time, "NS" was a member of the Ethiopian People's Revolutionary Party-Youth League when he was arrested at the age of 14. "NS" was beaten and threatened to be killed while imprisoned. The worst of the beatings occurred during the first two days when he was continuously beaten and tortured with an electric cattle prod. "NS" was shown a photographic lineup display, including the picture of "Habteab Berhe TEMANU." "NS" identified the photograph of "TEMANU" as a prison guard who participated in these beatings.
32. On February 21, 2012, S.B. was interviewed. S.B. admitted that the person who immigrated to the United States as his father, Habteab Berhe TEMANU, is an impostor and that his real father died in Asmara, Eritrea in 2005. S.B. stated that he has no knowledge of the real identity or biographical history of the impostor but knows that the impostor uses the nickname "TUFA." S.B. was shown a picture of "Habteab Berhe TEMANU" and he identified it as the impostor he knows as "TUFA" and not his father. Subsequently, S.B. provided a copy of his father's death certificate he obtained from the government of Eritrea which indicates Habteab Berhe TEMANU died on March 29, 2005.
33. S.B. explained that his real father had been born in what is present day Eritrea, which gained independence from Ethiopia in 1991. When Ethiopia and Eritrea went to war in approximately 1998, Ethiopia was a dangerous place for Ethiopians with Eritrean ancestry such as in the case of S.B.'s family. S.B. explained that at the time TEMANU's refugee application process began, his real father's health and mental state were deteriorating to the extent that the family did not feel he could successfully complete the required refugee interviews. S.B. and his siblings were concerned that their father's health would jeopardize their chances to immigrate to the United States. According to S.B., his siblings recruited "TUFA" to assume the identity of their father in the refugee process.

34. On April 4, 2012 and on May 29, 2012, A.B., one of the siblings who immigrated to the United States with "TUFA," was interviewed regarding his background and knowledge of "TUFA." A.B. confirmed that he and his siblings, Y.B., M.B., and T.B., fled Ethiopia for Kenya in approximately 2000 after the conflict between Ethiopia and Eritrea had escalated. Subsequently, S.B. sponsored his siblings to resettle in the United States. However, the family was concerned because their father was not well mentally. They feared if their father could not pass the refugee interview process they would lose their chance to resettle in the United States. Through an intermediary or broker who specialized in placing displaced individuals in "vacant refugee slots," A.B. was put in contact with "TUFA." "TUFA" told A.B. that he was a political refugee from Ethiopia and A.B. believed that "TUFA" had been in Nairobi for several years. "TUFA" studied A.B.'s family background and biographic information and assumed the identity of their father, Habteab Berhe TEMANU, throughout the refugee process. "TUFA" (using the TEMANU identity) and A.B. and his siblings were granted refugee status and immigrated to the United States on July 12, 2004.
35. On April 3, 2012, a naturalized United States citizen originally from Ethiopia (hereinafter referred to as "BD"), was interviewed by HSI agents in Sterling, Virginia. "BD" stated that he was arrested in Addis Ababa, Ethiopia in 1978, accused of being a political activist, and he was brought to the prison known as the "Higher 15." "BD" recalled that when he arrived at the prison, he was bound with wire type rope and tortured for eleven (11) or twelve (12) hours, enduring a severe beating with rifle butts, whips, and pipes. "BD" was imprisoned for approximately nine (9) months and sustained several of these beatings. At one point, a prison guard poured a liquid on his open wounds which caused severe pain and the guard put an AK-47 to his head, threatening to kill him. "BD" believes that many people held in the prison were executed. "BD" was shown a photographic lineup display, which included the picture of "Habteab Berhe TEMANU" ("TUFA"). "BD" identified the photograph of "TEMANU" as the person he knows as Kefelegn ALEMU, the prison guard who beat and tortured him, including pouring liquid on his open wounds and threatening his life with a rifle.
36. The residence located at 8861 E. Florida Avenue, Apartment B110, Denver, Colorado is located within the Sierra Vista apartment complex. The property manager recognized a photograph of "TEMANU" and confirmed that he has been a resident in this unit since 2009. Recent spot checks have confirmed the gold Toyota automobile, bearing Colorado license plates 472 OVL registered to "TEMANU," is routinely parked in front of 8861 E. Florida Avenue, Denver, Colorado. On July 3, 2012, I interviewed "TEMANU" under pretext and he confirmed that he has been a resident of 8861 E. Florida Avenue, Apartment B110, Denver, Colorado for approximately three (3) years. On August 13, 2012, a spot check was conducted on the Sierra Vista apartment complex and the gold Toyota registered to "TEMANU" was observed parked in its usual spot in front of building 8861 E. Florida Avenue.
37. Your affiant knows from experience with several search warrant executions and immigration fraud investigations that people tend to keep evidence of their true identity in their homes such as birth certificates, property information, photographs, correspondence, and information relating to their true family members. Your affiant also knows from experience that people who use assumed identities keep information relating to their assumed identity in their homes such as counterfeit or forged identity documents

and well as indicia of how the documents were obtained such photographs and applications.

38. On August 20, 2012, a two-count Indictment was returned by the federal grand jury sitting in Denver, Colorado, charging violations of Title 18 United States Code, Section 1425(a) and (b) [Procurement of Naturalization Unlawfully]; and Title 18, United States Code, Section 1028A(a)(1) [Aggravated Identity Theft].

CONCLUSION

39. Based on the preceding information, your affiant submits that there is probable cause to believe that an unidentified person known as “TUFA” also known as Kefelegn ALEMU has assumed the identity of Habteab Berhe TEMANU, a deceased citizen of Eritrea/Ethiopia. This unidentified person fraudulently applied for and received classification as a refugee to the United States using TEMANU’s identity and family biography. He subsequently filed fraudulent immigration forms in TEMANU’s name, specifically Form I-485, Application to Adjust Application to Register Permanent Residence or Adjust Status and Form N-400, Application For Naturalization, all in violation of Title 18 United States Code, Section 1425(a) and (b) [Procurement of Naturalization Unlawfully]; and Title 18, United States Code, Section 1028A(a)(1) [Aggravated Identity Theft]. Based on the foregoing, there is probable cause to additionally believe that he violated Title 18, United States Code, Section 1028(a)(3), (4), (7)[Fraud and related activity in connection with identification documents and information], and Title 18, United States Code, Section 1546(a)[Fraud and misuse of visas, permits, and other documents].

40. Based on the investigation described above, probable cause exists to believe that at the residence located at of 8861 E. Florida Avenue, Apartment B110, Denver, Colorado] (described on Attachment A), will be found evidence, fruits, and instrumentalities of a violation of Title 18 United States Code, Section 1425(a) and (b) [Procurement of Naturalization Unlawfully], Title 18, United States Code, Section 1028(a)(3), (4), (7)[Fraud and related activity in connection with identification documents and information],], Title 18, United States Code, Section 1028A [Aggravated Identity Theft] and Title 18, United States Code, Section 1546(a)[Fraud and misuse of visas, permits, and other documents]. (described on Attachment B).
41. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.

s/SA Jeffrey Lembke
Special Agent Jeffrey Lembke
HSI/ICE

Sworn to before me this 23rd day of August, 2012.


United States Magistrate Judge

Application for search warrant was reviewed and is submitted by Brenda Taylor, Assistant United States Attorney and Lillian Alves, Special Assistant United States Attorney.